FORM PTO-1390 (REV 12-29-99) U.S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER	
82032-0005	
U.S. APPLICATION NO (If known, see 37 CFR 1.5)	
09/763732	
INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE
PCT/EP99/06344	30 August 1999 (30.08.99)
PRIORITY DATE CLAIMED	
31 August 1998 (31.08.98)	

TITLE OF INVENTION: SYSTEM FOR PROVIDING ENCRYPTED DATA, SYSTEM FOR DECRYPTING ENCRYPTED DATA AND METHOD FOR PROVIDING A COMMUNICATION INTERFACE IN SUCH A DECRYPTING SYSTEM

APPLICANT(S) FOR DO/EO/US

Wilhelmus Gerardus Petrus MOOIJ and Andrew Augustine WAJS

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. X This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. X This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. X A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. X A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. X has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☐ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☐ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. X An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern document(s) or information included:

11. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. X An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. X A FIRST preliminary amendment.
    ☐ A SECOND or SUBSEQUENT preliminary amendment.
14. ☐ A substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. X Other items or information:
    -Courtesy copy of the International Application as published with International Search Report.
    -Courtesy copy of the International Preliminiary Examination Report.

The PTO did not rec[illegible]wing listed item(s) check $/;0 and assignment

U.S. APPLICATION NO. (If known, see 37 CFR 1.5) 09/763752	INTERNATIONAL APPLICATION NO PCT/EP99/06344	ATTORNEY'S DOCKET NUMBER 82032-00005

17. X The following fees are submitted:

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5):

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1,000.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepartd by the EPO or JPO **$860.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy Provisions of PCT Article 33(1)-(4) **$690.00**

International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4) **$96.00**

	CALCULATIONS PTO USE ONLY	
ENTER APPROPRIATE BASIC FEE AMOUNT =	$860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 X 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	15-20 =		X $18.00	$	
Independent claims	4- 3 =	1	X $80.00	$ 80.00	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+$260.00	$	
TOTAL OF ABOVE CALCULATIONS =				$940.00	
Reduction of 1/2 for filing by small entity, if applicable. A Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28).					
SUBTOTAL =				$940.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). +					
TOTAL NATIONAL FEE =				$940.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40.00	
TOTAL FEES ENCLOSED =				$980.00	
				Amount to be refunded:	$
				charged:	$

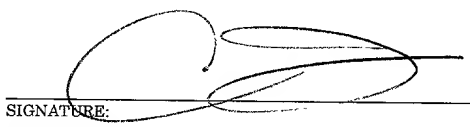
a. X A check in the amount of $980.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $_____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. X The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-1349. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO.
HOGAN & HARTSON LLP
Celine Jimenez Crowson
555-13th Street, N.W., 7W
Washington, D.C. 20004
(202) 637-5703



SIGNATURE:

CELINE JIMENEZ CROWSON
NAME

40,357
REGISTRATION NUMBER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
W.G.P. MOOIJ et al.	)	371 of International Application
Serial No.: **not yet assigned**	)	IA #: **PCT/EP99/06344**
Filed: **even date herewith**	)	IA Date: **30 August 99**
Title: **SYSTEM FOR PROVIDING ENCRYPTED DATA, SYSTEM... SUCH A DECRYPTING SYSTEM**	)	ATTY DKT NO.: **82032-00005**

PRELIMINARY AMENDMENT

Commisioner of Patents and Trademarks
Washington, D.C.

Sir:

Prior to calculation of the filing fee and examination on the merits, please amend the above-identified application as follows.

IN THE CLAIMS:

Claim 7, line 1, delete "5 or 6,".

Claim 8, line 1, change "anyone of claims 4-7" to --claim 4--.

Claim 9, line 1, change "any one of claims 4-8" to --claim 4--".

Claim 12, line 1, delete "or 11".

Claim 13, line 1, delete "or 11".

Claim 14, line 1, change "anyone of claims 10-13" to –claim 10--.

REMARKS

The above amendments are being made to delete multiple dependencies in the claims and does not add to or depart from the original disclosure or constitute prohibited new matter.

Respectfully submitted,

Celine ~~Jimenez~~ Crowson
Registration No. 40,357
Attorney for Applicant
Hogan & Hartson, LLP
555 13th Street, N.W., Suite 300-W
Washington, D.C. 20004
PH: 202-637-5600

System for providing encrypted data, system for decrypting encrypted data and method for providing a communication interface in such a decrypting system.

The invention generally relates to a system for providing encrypted data to be used in a content player, to a system for decrypting encrypted data in a content player, and to a method for providing a communication interface between a decryption device and a secure device in a content player. More particularly the invention relates to such systems and a method to create an open access interface for a wide range of multimedia terminals.

In the present specification the term "content player" is meant to indicate any type of consumer equipment, such as a (digital) TV set, a set top box, a DVD player or a (digital) VCR. In order to allow access to contents, such as a movie, football match, etc., it is known to protect the contents by encryption of the data using a suitable encryption algorithm. Subscribers are provided with a set top box for example and a secure device, wherein the secure device generates information necessary to decrypt the encrypted data. Conventional systems of this type are provided with a fixed interface and protocols for communication between the secure device and the content player. A fixed interface shows the disadvantage that the content player can only be used with one or more specific secure devices.

The invention aims to provide systems and a method of the above-mentioned type allowing to create a variable interface between the secure device and a content player.

According to a first aspect of the invention, a system for providing encrypted data to be used in the content

player is provided, comprising an encryption device for encrypting data using an encryption algorithm, a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device, and a control device for providing a protected contents containing the encrypted data, the secure device data, said protocol information and attribute data on the different parts inside the protected contents.

According to a second aspect of the invention, a system for decrypting encrypted data in a content player is provided, comprising an input for receiving a protected contents containing the encrypted data, secure device data, information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, a decryption device and a control device, wherein the control device is programmed to use said protocol information to establish a communication interface between the decryption device and a secure device used with the contents player, wherein the decryption device is adapted to communicate with the secure device as controlled by the protocol information to obtain information required to decrypt the encrypted data.

According to a further aspect of the invention, a method for providing a communication interface between a decryption device in a content player and a secure device is provided, comprising receiving a protected contents containing information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, retrieving said protocol information from the protected contents to establish a communication interface between the decryption device and a secure device used with the contents player.

According to a still further aspect of the invention a method for transmitting or the like of encrypted data is provided, wherein the encrypted data is obtained by means of the system for providing encrypted data according to the invention.

In this manner the invention provides a variable interface platform, wherein any communication interface between a secure device and content player can be established. The invention allows content protection technology to be adapted and to maintain interoperability with existing technology used in present consumer equipment. In this manner backwards compatibility in content protection systems and secure device interfaces is obtained.

The invention will be further explained by reference to the drawings in which an embodiment of the systems of the invention applying the method of the invention are shown in a schematical manner.

Fig. 1 shows an in-home distribution network interconnecting a number of consumer content players.

Fig. 2 shows a diagram of the architecture of an embodiment of the system for providing encrypted data to be used in a content player according to the invention.

Fig. 3 shows a diagram of the architecture of an embodiment of the system for decrypting encrypted data in a content player according to the invention.

By way of example fig. 1 shows an in-home distribution netwerk 1 interconnecting a plurality of content player devices such as a TV set 2, a DVD player 3, a DVCR 4 and a PC 5. Further a camcorder 6, a set top box (STB) 7 and a secure device 8, such as for example a smart card, are connected to the network 1. Finally the network is linked to a wide area network, such as the internet, as indicated by reference nu-

meral 9. In this example of an in-home distribution network 1, the STB 7 and the secure device 8 communicate through a communication interface in order to decrypt any encrypted data obtained from protected contents as will be described later. The STB 7 and secure device 8 are common to the content players 2-5 in this example, although it is also possible that each of the content players is provided with its own decoder/decryption device communicating with its own secure device. It is noted that protected contents can be moved through the network 1 to a target content player using a suitable protocol and adressing technique which are not part of the present invention.

Fig. 2 shows a system for providing encrypted data to be used in a content player, comprising an encryption device 10, a protection device 11 and a control device 12 including a multiplexer 13. Clear contents, such as a movie, a football match, etc., is encrypted in the encryption device 10 using a suitable encryption algorithm. In the encryption algorithm keys are used which are provided by the protection device 11 and these keys are themselves encrypted in one or more formats by the protection device 11. The encrypted keys are provided as secure device data. The protection device 11 further provides information on a protocol for communication between the content player and the secure device 8. In the embodiment shown, the information on the protocol and encryption format(s) is provided as one or more secure device applets.

The encrypted contents provided by the encryption device, the secure device applet(s) and the secure device data are multiplexed into protected contents, also containing attribute data provided by the control device 12. The attribute data are required to find the relevant parts inside the

protected contents structure. The output of the multiplexer 13 can be broadcast for example or stored on a suitable medium for later use.

The system shown in fig. 2 may be adapted to handle one or more different secure device formats and for each of these formats the protection device 11 provides a secure device applet. The main funtion of the secure device applet is to implement in the content player the protocol and format to communicate with the secure device connected to the content player. In this manner it is possible to provide an interface between the secure device and the content player without specific knowledge beforehand of the protocol required by the specific secure device used.

Preferably each secure device applet is authenticated, for example by a signature which shows that it originated from a legitimate source. Suitable public key cryptographic hashing functions can be used.

Fig. 3 shows a system for decrypting encrypted data in a content player as shown, comprising an input 14 for receiving protected contents, a decryption device 15 and a control device 16 including a demultiplexer 17. A secure device 8 is connected to the control device 16. Further a decoder 18 is shown for decoding decrypted data in a manner known per se. The decoder 18 is not part of the present invention. The attribute data is used in the control device 16 to demultiplex the protected contents to retrieve a secure device applet or applets, the secure device data and the encrypted contents and to forward the respective parts of the contents to the corresponding components of the content player.

In order to decrypt the encrypted contents, the content player needs to retrieve the keys from the secure device 8. To this end the control device 16 determines the type

of secure device 8 connected to the content player and searches the attribute data to select the appropriate corresponding security device applet. The control device 16 includes an applet loader 19 to verify the signature of the secure device applet. If the secure device applet is verified, this applet is downloaded in a virtual machine programmed into the control device and is executed in this environment to establish a communication interface between the secure device 8 and the content player and decryption device 15. Once the communication interface is established, the secure device applet operates to fetch the secure device data from the protected contents which is tranformed by the secure device 8 into the keys required by the decryption device 15 to decrypt the encrypted contents.

As noted, the applet loader 19 verifies whether the secure device applet is an authentic one. In this manner the applet loader restricts access to the virtual machine to those applets originating from an authentic source. A standard method to achieve verifying of the secure device applet is authentication using a public key cryptographic hashing function. Optionally, the applet may be encrypted using a conventional secret key cryptographic algorithm. The attribute data contains fields specifying both the type of cryptographic algorithm and secret key index to be used in the signature verification process.

In the virtual machine, the secure device applet uses a content player application program interface to communicate with the content player on the one side and a security application program interface to communicate with the secure device 8 and the decryption device 15.

The control device 12 is arranged to indicate in the attribute data the type of secure device 8 supported in

the content player. When the secure device 8 has been determined, for example by finding the unique identifier in a manner known per se, the secure device applet corresponding with the secure device by virtue of having a matching identifier is selected from the attribute data. On the basis of this information, the applet loader retrieves the secure device applet from the protected contents. This process will generally be used in an application, wherein the protected contents is received in a continuous stream in case of a broadcasting environment for example. The same process can be used when the protected contents is stored on a tape or disc. In case of an broadcasting environment or wide area network, it is also possible for the applet loader 19 to request a service provider or the like to forward a secure device applet corresponding to the detected type of secure device.

It is observed that the security of the system described is at least as good as any existing security system. As the protected contents is always encrypted until it reaches the target content player, it is difficult to obtain a clear text version of the contents. Moreover the flexibility of the system described allows for defense and counter measures against presently existing attacking techniques, which counter measures are not available in existing protection systems.

It is noted that the term "content player" should be understood as to mean any device mentioned above or even a separate decoder equipment having an interface for the secure device. Further it is noted that although wording is used in the above description suggesting separate devices in the systems decribed, it will be clear that both the encrypting and decrypting system can be implemented by means of a micropro-

cessor and suitable peripheral circuits operating in the manner described as controlled by suitable software.

The system described supports a wide range of applications. As already mentioned, a first application area is a broadcasting environment. The content player in this case can be a set top box connected to a TV or a DVCR. The virtual machine can be implemented using JAVA. Generally an ISO 7816 smart card is used as secure device. According to a favourable embodiment, it will also be possible for non-subscribers to buy a specific "event", such as a football match, using a standard banking card, wherein the applet loader requests the service provider to download a suitable secure device applet. Other applications are pre-recorded media, such as CD, DVD, DVCR tapes and other cassettes. In the described system of the invention, the stored protected contents includes a number of supported secure device applets, so that the applet loader of the control device can retrieve the secure device applet corresponding with the secure device used in the specific content player. In this manner again backwards compatibility is allowed, whereas future upgrades can be made in a flexible manner.

The invention is not restricted to the above-described embodiments which can be varied in a number of ways within the scope of the following claims.

CLAIMS

1. System for providing encrypted data to be used in a content player, comprising an encryption device for encrypting data using an encryption algorithm, a protection device for providing secure device data, and for providing information on a protocol for communication between the content player and a secure device, and a control device for providing a protected contents containing the encrypted data, the secure device data, said protocol information and attribute data on the different parts inside the protected contents.

2. System according to claim 1, wherein said protection device provides at least one secure device applet containing said information on a protocol for communication.

3. System for decrypting encrypted data in a content player, comprising an input for receiving encrypted data containing encrypted contents, secure device data, information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, a decryption device and a control device, wherein the control device is programmed to use said protocol information to establish a communication interface between the decryption device and a secure device used with the content player, wherein the decryption device is adapted to communicate with the secure device as controlled by the protocol information to obtain information required to decrypt the encrypted data.

4. System according to claim 3, wherein said protocol information is provided as a secure device applet, whe-

rein the control device is programmed to operate as a virtual machine to execute the secure device applet to establish said communication interface.

5. System according to claim 3, wherein at least one secure device applet in the protected contents is authenticated, wherein the control device comprises an applet loader for verifying the authentication of a secure device applet, wherein only a verified secure device applet is loaded into the virtual machine.

6. System according to claim 5, wherein at least one secure device applet in the protected contents is encrypted, wherein the applet loader is adapted to decrypt an encrypted secure device applet.

7. System according to claim 4, 5 or 6, wherein the virtual machine comprises a content player application program interface and a security application program interface, the secure device applet communicating with the content player and the secure device by means of said interfaces.

8. System according to anyone of claims 4-7, wherein the control device is arranged to determine the type of secure device used in the system, wherein the control device is arranged to retrieve a secure device applet from the protected contents corresponding with the type of secure device.

9. System according to anyone of claims 4-8, wherein the system is part of a content player connected to a network, wherein the control device is arranged to determine the type of secure device used in the system, and wherein the control device is arranged to request a corresponding secure device applet to be downloaded from a service provider.

10. Method for providing a communication interface between a decryption device and a secure device in a content player, comprising receiving a protected contents containing

information on a protocol for communication between the content player and a secure device, and attribute data on the different parts inside the protected contents, retrieving said protocol information from the protected contents to establish a communication interface between the decryption device and a secure device used with the contents player.

11. Method according to claim 10, wherein said protocol information is provided as a secure device applet, wherein the secure device applet is executed in a virtual machine to establish the communication interface.

12. Method according to claim 10 or 11, further comprising detecting the type of secure device used with the content player, and retrieving corresponding protocol information or a secure device applet from the protected contents.

13. Method according to claim 10 or 11, further comprising detecting the type of secure device used with the content player, and requesting corresponding protocol information or a secure device applet from a source providing the protected contents.

14. Method according to anyone of claims 10-13, wherein said protocol information or secure device applet is authenticated, further comprising verifying the authentication, and using only verified protocol information or a verified secure device applet to establish said communication interface.

15. Method for transmitting or the like encryted data obtained by means of a system according to claim 1 or 2.

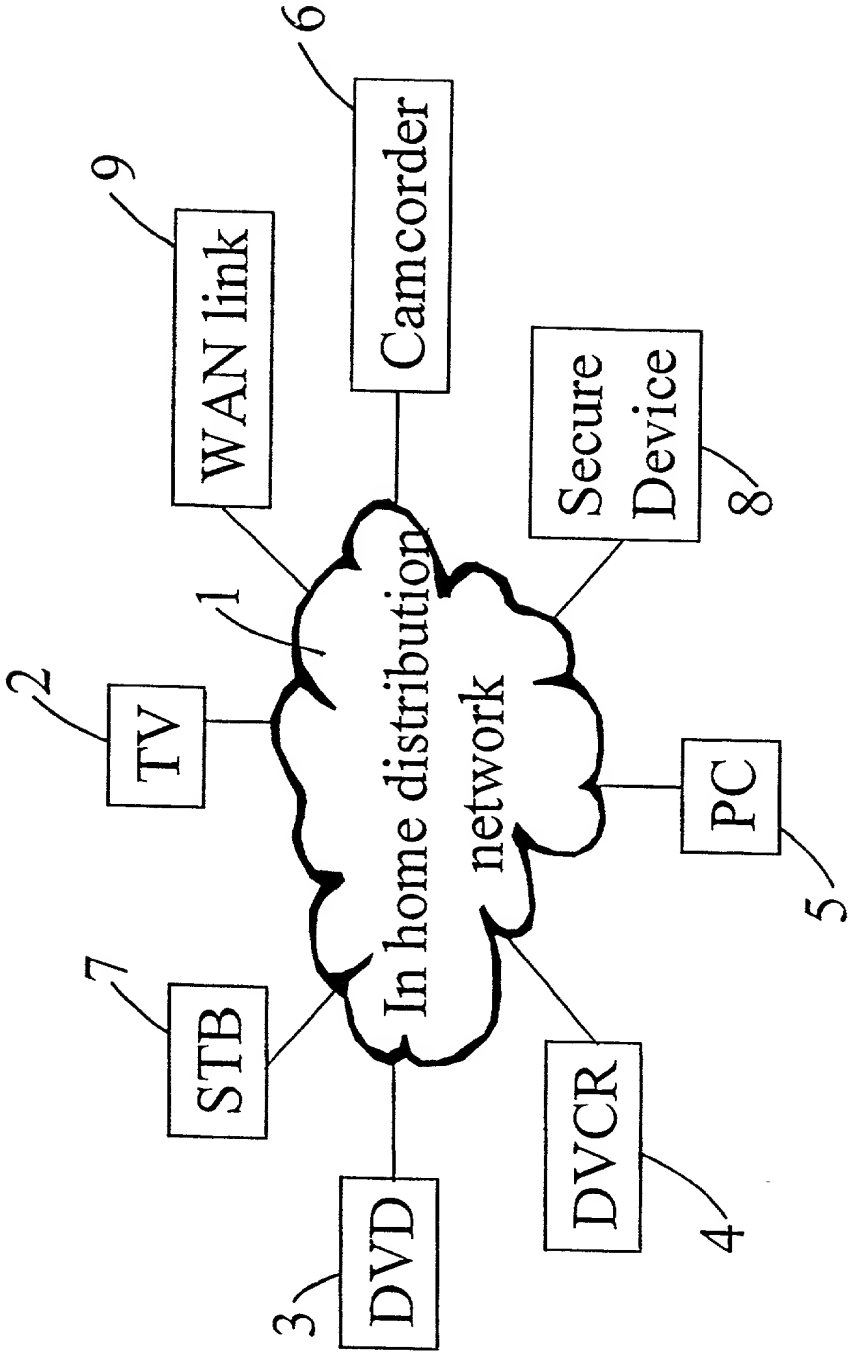

In home distribution network
1
TV
2
DVD
3
DVCR
4
PC
5
STB
7
Secure Device
8
WAN link
9
Camcorder
6

Fig. 1

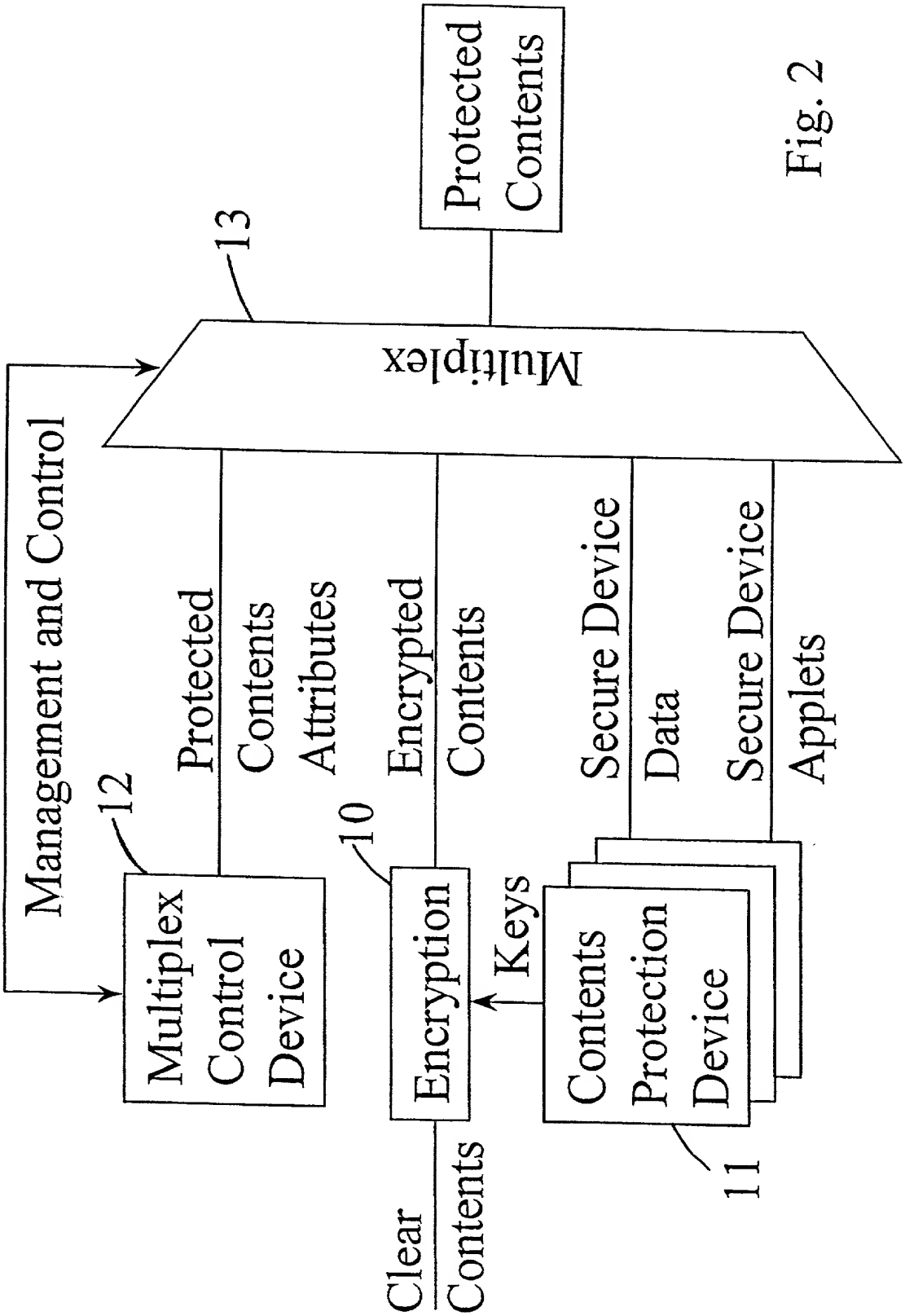

Protected Contents
13
Multiplex
Management and Control
12
Multiplex Control Device
Protected Contents Attributes
10
Encryption
Keys
Encrypted Contents
Contents Protection Device
11
Secure Device Data
Secure Device Applets
Clear Contents

Fig. 2

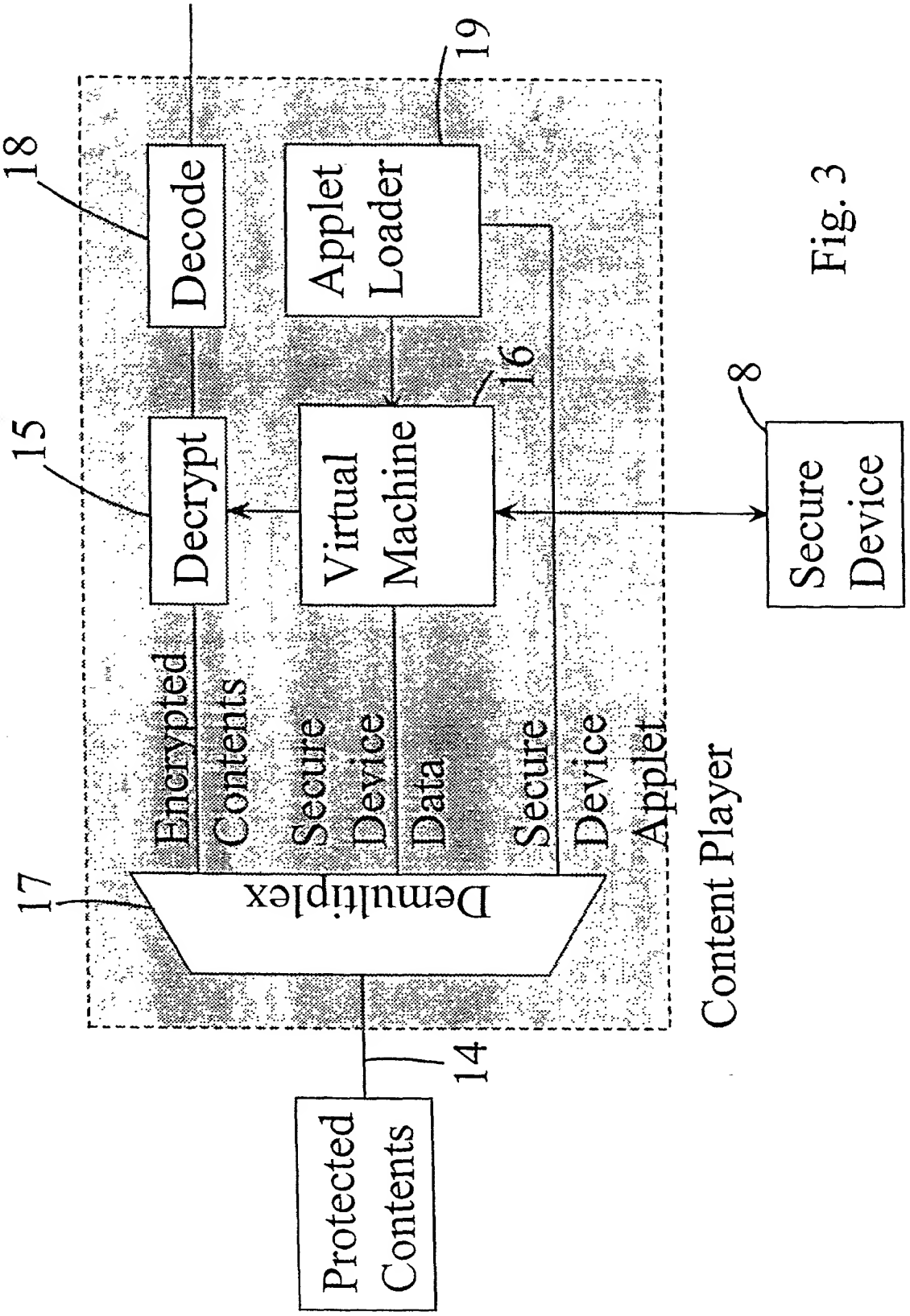

Protected Contents
14
Content Player
Demultiplex
17
Encrypted Contents
Secure Device Data
Secure Device Applet
Decrypt
15
Virtual Machine
16
Decode
18
Applet Loader
19
Secure Device
8

Fig. 3

Docket No. 82032-00005

Declaration and Power of Attorney for Patent Application

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought, on the invention entitled **SYSTEM FOR PROVIDING ENCRYPTED DATA, SYSTEM FOR DECRYPTING ENCRYPTED DATA AND METHOD FOR PROVIDING A COMMUNICATION INTERFACE IN SUCH A DECRYPTING SYSTEM**, the specification of which is attached hereto as Attorney Docket No. 82032-00005.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

		Priority Claimed		
98202891.2 ✓	Europe ✓	31 August 98 ✓	[x]	[ ]
(Number)	(Country)	(Day/Month/Year)	Yes	No

I hereby claim the benefit under Title 35, United States Code § 119(e) of any United States provisional application(s) listed below.

_____ _____

(Application Serial No.) (Filing Date)

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose

material information as defined in Title 37, Code of Federal Regulations, 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

PCT/EP99/06344	30 August 1999	
(Application Serial No.)	(Filing Date)	(Status)

I or we hereby appoint the following attorneys to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and request that all correspondence about the application be addressed to HOGAN & HARTSON L.L.P., 555 13th Street, N.W., Washington, D.C. 20004, Customer No. 24633

2 – Celine Jimenez Crowson, Reg. No. 40,357
Kevin G. Shaw, Reg. No. 43,110

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

FIRST NAMED INVENTOR	SIGNATURE	DATE
1 Wilhelmus Gerardus Petrus MOOIJ	Wim Mooij	5 feb 2001
RESIDENCE	CITIZENSHIP	
NL-1115 DK Duivendrecht.	The Netherlands NLX	
POST OFFICE ADDRESS		
Basilicum 7, NL-1115 DK Duivendrecht, The Netherlands		
SECOND NAMED INVENTOR	SIGNATURE	DATE
2 Andrew Augustine WAJS.	A A Wajs	2/02/2001
RESIDENCE	CITIZENSHIP	
NL-2023 AA Haarlem	Great Britain GBN	
POST OFFICE ADDRESS		
Schotersingel 93, NL-2023 AA Haarlem, The Netherlands		